U.S. Department of Justice

Richard P. Donoghue
United States Attorney
Eastern District of New York

271 Cadman Plaza East
Brooklyn, New York 11201

FOR IMMEDIATE RELEASE **September 25, 2019**

Contact:
John Marzulli
United States Attorney's Office
(718) 254-6323

PRESS RELEASE

TWO KAZAKH CYBERCRIMINALS PLEAD GUILTY IN GLOBAL DIGITAL ADVERTISING FRAUD INVOLVING TENS OF MILLIONS OF DOLLARS IN LOSSES

Leader of Scheme Will Forfeit Online Domains and More Than Eight Million Dollars Seized From Swiss Bank Accounts

Sergey Ovsyannikov and Yevgeniy Timchenko, citizens of the Republic of Kazakhstan, pleaded guilty yesterday and today, respectively, in federal court in Brooklyn to conspiring to commit wire fraud and related charges, for their involvement in a widespread digital advertising fraud. Ovsyannikov was arrested in October 2018 in Malaysia and extradited to the United States in March 2019. Timchenko was arrested in November 2018 in Estonia and extradited to the United States in February 2019. Both plea proceedings took place before United States Magistrate Judge Steven M. Gold. When sentenced, Ovsyannikov faces up to 42 years in prison, and Timchenko faces up to 40 years in prison.

Richard P. Donoghue, United States Attorney for the Eastern District of New York, and William F. Sweeney, Jr., Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI), announced the guilty pleas.

Background on Digital Advertising

The internet is, in large part, freely available to users worldwide because it runs on digital advertising, where website owners display advertisements on their sites and are compensated by intermediaries representing businesses that advertise goods and services to human customers. In general, digital advertising revenue is based on how many users click, or view, the advertisements on those websites. As alleged in court filings, the defendants in this case represented that they ran legitimate companies that delivered advertisements to human internet users, who accessed real internet webpages. In fact, the defendants faked both the users and the webpages they programmed computers they controlled to load advertisements on fabricated webpages, via an automated program, and fraudulently obtained digital advertising revenue.

The Botnet-Based Criminal Scheme ("3ve.2 Template A")

Between December 2015 and October 2018, Ovsyannikov and Timchenko were involved in operating a purported advertising network and carried out a digital advertising fraud scheme, referred to in the advertising industry as "3ve.2 Template A." In this scheme, the defendants used a global "botnet"— a network of malware-infected computers operated without the true owner's knowledge or consent to perpetrate their fraud. The defendants developed an intricate infrastructure of command-and-control servers to direct and monitor the infected computers, and to detect whether a particular infected computer had been flagged by cybersecurity companies as being associated with fraud. By using this infrastructure, the defendants accessed more than 1.7 million infected computers belonging to individuals and businesses in the United States and elsewhere, and used hidden browsers on those infected computers to download fabricated webpages and load advertisements onto those fabricated webpages. Meanwhile, the owners of the infected computers were unaware that this process was running in the background on their computers. As a result of this scheme, the defendants falsified billions of advertisement views and caused businesses to pay more than $29 million for advertisements that were never actually viewed by human internet users.

The Defendants' Roles

Ovsyannikov led the development of the 3ve.2 scheme, and was a principal and owner of the advertisement network used to carry out the scheme. Ovsyannikov set out the infrastructure of the scheme in a spreadsheet titled "[Ad Network] Structure. Hosting and Domains." The spreadsheet listed many of the command-and-control servers and other servers involved in the scheme, including several designated as repositories of "spoof" webpages. Ovsyannikov maintained lists of webpages to fabricate (or "spoof") in his cloud storage account and on servers that he controlled, including more than 86,000 webpages associated with online publishers, including the webpages of thousands of businesses in the United States. In communications with co-conspirators, Ovsyannikov explained how different aspects of the infrastructure worked together to perpetrate the fraud, such that a "bot" in the botnet would "set itself" to visit a "spoofed domain" and cause a falsified advertisement view. Ovsyannikov directed proceeds of the fraud to bank accounts in Switzerland, among other locations. As part of his guilty plea, Ovsyannikov will forfeit those Swiss bank accounts, which contain more than eight million dollars.

Timchenko worked for Ovsyannikov and handled logistical and administrative aspects of the 3ve.2 scheme. Timchenko assisted in creating the infrastructure of command-and-control servers and other servers that were instrumentalities of the scheme. Timchenko deliberately chose certain U.S. service providers because they had the "coolest processors" and a "larger" cache (for temporary data storage) than competing providers. Timchenko also researched webpages to fabricate, deliberately targeted webpages for businesses in the United States, and placed those webpages on a running list that both defendants kept that was titled "New companies for spoofing."

Separately, Ovsyannikov provided technical assistance to the operators of another digital advertising fraud scheme, referred to in the advertising industry as "Methbot." In the

Methbot scheme, the perpetrators used computers housed in commercial datacenters, instead of in a botnet, to carry out the digital advertising fraud. Ovsyannikov helped the Methbot operators program the datacenter computers to mimic human behavior, disguise the computers' automated browsers, and evade fraud detection software. The Methbot operators falsified billions of advertisement views and caused businesses to pay more than $7 million for advertisements that were never actually viewed by human internet users.

The Botnet Takedown

Following the arrest of Ovsyannikov by Malaysian authorities in October 2018, U.S. law enforcement authorities, in conjunction with various private sector companies, began the process of dismantling the criminal cyber infrastructure utilized in the botnet-based scheme, which involved computers infected with malicious software known "Kovter." The FBI executed seizure warrants to redirect the internet traffic going to 23 internet domains used to further the charged botnet-based scheme or otherwise used to further the Kovter botnet (an action known as "sinkholing"), in order to disrupt and dismantle the botnet. The FBI also executed search warrants at 11 different U.S. server providers for 89 servers related to the charged botnet-based scheme or Kovter.

In addition, as part of its investigation, the FBI discovered an additional cybercrime infrastructure committing digital advertising fraud through the use of datacenter servers located in Germany, and a botnet of computers in the United States infected with malicious software known in the cybersecurity community as "Boaxxe." The FBI executed seizure warrants to sinkhole eight domains used to further this scheme and thereby disrupt yet another botnet engaged in digital advertising fraud.

Finally, the United States, with the assistance of its foreign partners, executed seizure warrants for multiple international bank accounts in Switzerland and elsewhere that were associated with the schemes.

For technical details on the malware and botnets referenced in this case, please see US-CERT Alert TA18-331A: https://www.us-cert.gov/ncas/alerts/TA18-331A

The government's case is being prosecuted by the Office's National Security and Cybercrime Section. Assistant United States Attorneys Saritha Komatireddy, Michael T. Keilty, Alexander F. Mindlin and Karin K. Orenstein are in charge of the prosecution.

The Defendants:

SERGEY OVSYANNIKOV
Age: 30
Republic of Kazakhstan

YEVGENIY TIMCHENKO
Age: 31
Republic of Kazakhstan